

Abstract of the Invention

A high-speed, low-strength authentication mechanism is disclosed. This mechanism is based on a partial message authentication code, wherein a message authentication code is applied only to some portion of the message. By applying an authentication algorithm only to selected parts of the message, significant time can be saved while maintaining acceptable security.

THE JOURNAL OF THE